UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,312	03/17/2005	Markus Franke	2002P15289WOUS	2692

7590   10/18/2007

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, NJ 08830

EXAMINER
HAILU, TESHOME

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
10/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>17 March 2005</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>6-23</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>6-23</u> is/are rejected.

7)☒ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>17 March 2005</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☒ All   b)☐ Some * c)☐ None of:

   1.☒ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date <u>03/17/2005</u>.

4)☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-5 are canceled.

2.   Claims 6-23 are pending.

Claim Objections

3.   Claims 16 and 17 are objected to under 37 CFR 1.75(c), as being of improper dependent

form for failing to further limit the subject matter of a previous claim. Both claims are equivalent

each other. Applicant is required to cancel the claim(s), or amend the claim(s) to place the

claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section
> 122(b), by another filed in the United States before the invention by the applicant for patent or
> (2) a patent granted on an application for patent by another filed in the United States before
> the invention by the applicant for patent, except that an international application filed under
> the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an
> application filed in the United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English language.

5.   Claims 6-7, 12-13, 18-19 and 23 are rejected under 35 U.S.C. 102(e) as being

anticipated by Dierks et al (Dierks), US 6,948,061.

As per claims 6 and 18, Dierks discloses:

A method for generating and/or validating electronic signatures, the method comprising:

(column 5, line 19-20, "FIG. 4 details the manner in which a signature is validated using the

system 10 illustrated in FIGS. 1 and 2").

Generating an asymmetrical key pair which includes a private signature key and a public validation key; (column 6, line 46-49, "The secure token 12 attestation is accomplished prior to delivery to the end user in a secure domain. The secure token 12 is asked to generate a key pair comprising the token secure key 30 and a corresponding public key").

Calculating an electronic signature for an electronic document by means of the private signature key and by applying a predeterminable signature function: (column 6, line 29-32 "The validation engine 20 receives the authorization and enables the cryptographic engine 26 within the secure token 12 to execute the original request 112, creating a digital signature utilizing the private key").

Performing a certification of the public validation key. (Column 1, line 26-28, "The public key has been certified by a Certificate Authority (CA), which has issued the certificate C.sub.A"). Further Dierks disclosed, (column 9, line 42-44, "The use of the private key corresponding to a certified public key is based on the ongoing validity of the certificate").

As per claims 7 and 19, Dierks discloses:

The method according to Claim 6, wherein, when validating, only those signatures which are and/or were generated at a time prior to the certification of the public validation key are recognized as valid. (Abstract, line 1-5, "A certificate validity verification engine is integrated into the logic of a secure token, in turn, making the use of a private key conditional upon the determination that the certificate for the corresponding public key is valid at that particular instant in time").

As per claims 12-13 and 23, Dierks discloses:

The method according to Claim 6, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document. (Column 5, paragraph 29-35, "The validation engine 20 receives the authorization and enables the cryptographic engine 26 within the secure token 12 to execute the original request 112,

creating a digital signature utilizing the private key ".alpha.". Once the message is signed, the

certificate 22 is appended and returned to the application 114. In turn the application 14 sends

the certificate 22 onto the user 116"). Further Dierks teaches (column 3, line 9-12, "In the case

where a relying party is sending a message, the relying party determines that a certificate is valid,

encrypts the message, and sends it").

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described
> as set forth in section 102 of this title, if the differences between the subject matter sought to
> be patented and the prior art are such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person having ordinary skill in the art to which
> said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

7.   Claims 8-11, 14-17 and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Dierks, US 6,948,061, and further in view of Watanabe, US Pub. No. 2002/0108041.

As per claims 8-9 and 20-21, Dierks discloses:

The method according to Claim 6, wherein, when certifying the public validation key, a

reference to the electronic document is included in addition to a user identifier and the public

validation key. (Column 6, line 46-53, "The secure token 12 attestation is accomplished prior to

delivery to the end user in a secure domain. The secure token 12 is asked to generate a key pair

comprising the token secure key 30 and a corresponding public key. It stores the private key

secure and within the token, using it only in the token attestation process. The corresponding

public key is taken and certufued by a CA").

Dierks dose not explicitly discloses, a reference to the electronic document and user

identifier. On the other hand, on the same field of endeavor, Watanabe teaches this limitation as,

(page 1, paragraph 10, "A public key certificate is issued by a certificate authority (CA) or an

issuer authority (IA) in the public key cryptosystem. The public key certificate is prepared by user's submitting his ID and public key for example to a certificate authority and certificate authority's attaching its ID and validity for example and its signature to the information submitted by the user"). Further Waanabe disclosed, (page 1, paragraph 11, "The public key cryptosystem shown in FIG. 1 includes certificate's version number, certificate's serial number allocated by a certificate authority to a certificate's user, the algorithm and parameter of the above-mentioned RSA or ECC used for digital signature, the name of the certificate authority, certificate's validity, the name (user ID) of user of the certificate authority, and the public key and digital signature of this user").

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Dierks and include the document reference and user identifier in the process of certifying the public key using the teaching of Watanabe. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation and have a better certifying system.

As per claims 10-11 and 22, Dierks discloses:

The method according to Claim 8, wherein an implementation of the reference is performed by a calculation of a hash value for the electronic document. (Column 6, line 46-53, "The secure token 12 attestation is accomplished prior to delivery to the end user in a secure domain. The secure token 12 is asked to generate a key pair comprising the token secure key 30 and a corresponding public key. It stores the private key secure and within the token, using it only in the token attestation process. The corresponding public key is taken and certufued by a CA").

Dierks dose not explicitly discloses, the way of reference is performed. On the other hand, on the same field of endeavor, Watanabe teaches this limitation as, (page 2, paragraph 12, "the digital signature consists of data generated by generating a hash value on the basis of a hash function and applying the private key of the certificate authority to the generated hash value"). Further Watanabe teaches the above limitation in FIG. 1. (See Fig. 1).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Dierks and include a hash value to certify public key using the teaching of Watanabe. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation and have a better certifying system.

As per claims 14-17, Dierks discloses:

The method according to Claim 8, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document. (Column 5, paragraph 29-35, "The validation engine 20 receives the authorization and enables the cryptographic engine 26 within the secure token 12 to execute the original request 112, creating a digital signature utilizing the private key ".alpha.". Once the message is signed, the certificate 22 is appended and returned to the application 114. In turn the application 14 sends the certificate 22 onto the user 116"). Further Dierks teaches (column 3, line 9-12, "In the case where a relying party is sending a message, the relying party determines that a certificate is valid, encrypts the message, and sends it").

Conclusion

8.   The prior art made or record and not relied upon is considered pertinent to applicant's disclosure

TITLE: System and method for electronic transmission, storage, and retrieval of authenticated electronic original documents, US Pub. No. 2001/0002485.

TITLE: System and method for authentication in a crypt-system utilizing symmetric and asymmetric crypto-keys, US Pub. No. 2002/0078345.

TITLE: Systems and methods for secure transaction management and electronic rights protection, US 7,069,451.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Teshome Hailu whose telephone number is (571) 270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

October 11, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100